Amendments to the Claims

1. (previously amended) A method comprising:

receiving, at a BIOS in a system, a message from an authorized party, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor;

authenticating that the message has been sent by the authorized party using a digital signature in the message and a public key stored in non-volatile storage communicatively coupled to the BIOS;

verifying that the system is an intended recipient of the message, wherein verifying comprises comparing an identifier in the message against a globally unique identifier (GUID) of the system, the GUID stored in the non-volatile storage communicatively coupled to the BIOS; and

when the message has been successfully authenticated and verified,

controlling a state of an optional feature of a system resource in the system, using the BIOS, according to the message, wherein the message comprises information to determine the optional feature, and wherein the message further comprises a digital signature used for authenticating, and

when the message fails the authenticating or the verifying, then discarding the message.

2. (canceled)

3. (original) The method of claim 1 further comprising writing the message into a secure non-volatile location.

4. (original) The method of claim 3 wherein the secure non-volatile location comprises a remote storage.

5. (previously amended) The method of claim 1 further comprising splicing the content of the message into an execution path of the BIOS, wherein the splicing comprises at least one of modifying the BIOS or erasing a portion of the BIOS, in response to the message.

6. (previously amended) The method of claim 1 further comprising loading and executing content of the message using the BIOS at run-time, wherein the message is received via a network transmission.

7. (previously amended) The method of claim 1 further comprising updating a feature set of the system BIOS according to the message, wherein the feature set comprises a status of features of the system.

8. (previously amended) A system comprising:

a system resource having controllable optional features;

a non-volatile memory that stores a BIOS, the BIOS being adapted to receive a secure message from an authorized party for controlling at least one of the optional features, wherein the secure message comprises information to determine the at least one of the optional features, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor, and wherein the system is to boot without enabling the at least one optional feature when the secure message is not received from the authorized party; and

verification component to compare an identifier in the message against a globally unique identifier (GUID) of the system to verify an intended recipient of the message.

9. (previously amended) The system of claim 8 further comprising a write-once non-volatile unit for storing a public key accessible by the BIOS.

10. (previously amended) The system of claim 8 wherein the BIOS includes authentication circuitry for authenticating the secure message with a public key.

11. (previously amended) The system of claim 8 further comprising a write-once non-volatile unit for storing the GUID accessible by the BIOS.

12. (canceled)

13. (previously amended) The system of claim 8 further comprising a secure non-volatile location for storing at least one of the optional features to be enabled, the location being readable and writable by the BIOS.

14. (previously amended) The system of claim 13 wherein the location comprises a remote storage.

15. (previously amended) The system of claim 8 wherein the BIOS also includes a feature set that is updated according to content of the secure non-volatile storage, wherein the feature set comprises a status of features of the system.

16. (previously amended) The system of claim 8 wherein the BIOS loads and executes the content of the message at run-time, wherein the message is received via a network transmission.

17. (previously amended) A computer program product residing on a computer readable medium comprising instructions for causing a computer to:

receive, at a BIOS in a system, a message from an authorized party, wherein the authorized party is selected from a group of authorized parties consisting of a manufacturer, an original equipment manufacturer, and a lessor;

authenticate that the message has been sent by the authorized party using a digital signature in the message and a public key stored in a non-volatile storage communicatively coupled to the BIOS;

verify that the system is an intended recipient of the message, wherein verifying